REMARKS/ARGUMENTS

Applicant respectfully requests reconsideration and allowance of the subject application.

Claims 1-33 were originally submitted.

Claims 1, 19, 20 and 29 are currently amended.

No claims are canceled.

No new claims have been added.

Claims 1-33 remain in this application.

35 U.S.C. §101

Independent Claims 1, 7, 15, 19, 21 and 29 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The dependent claims are further rejected based on their dependencies on the rejected base claims. Applicant respectfully traverses the rejection.

Claim 1 has been amended to address this rejection. Claims 2-6 depend upon claim 1, and overcome the objection based on their dependence to the amended claim 1.

Claim 29 has been amended to address this rejection. Claims 30-33 depend upon claim 29, and overcome the objection based on their dependence to the amended claim 29.

Claims 7, 19, 21 are method claims which fall under fall under process claims and therefore are statutory subject matter. Claim 15 is directed to computer-readable medium having stored there on an object. Therefore, claim 15 is directed to functional descriptive material recorded on some computer-readable medium. Hence, claim 15 becomes structurally and functionally interrelated to the medium and is statutory. Claims 8-14 depend upon claim depend upon claim 7, and overcome the objection based on their dependence to the claim 7. Claims 16-18 depend upon claim depend upon claim 15, and overcome the objection based on their dependence to the amended claim 15. Claim 20 depends upon claim depend upon claim 19, and overcome the objection based on its dependence to the claim 19. Claims 22-28 depend upon claim depend upon claim 21, and overcome the objection based on their dependence to the amended claim 21.

Therefore, Applicant respectfully requests that the 35 U.S.C. §101 rejection of claims 1-33 be withdrawn.

35 U.S.C. §112

Independent Claims 19 and 20 are rejected under 35 U.S.C. 112 because the recite a trademark/trade name. Claims 19 and 20 have been amended to overcome the rejection. Therefore, Applicant respectfully requests that the 35 U.S.C. §112 rejection of claims 19 and 20 be withdrawn.

35 U.S.C. §102

Claims 1-33 have been rejected under 35 U.S.C. 102(b) as being anticipated by Jensenworth et al, United States Pat. No. 6,279,111 (Jensenworth). Applicant respectfully traverses the rejection.

Jensenworth teaches an improved security model for computer system. The model provides restricted access tokens, each of which are modified, restricted version of an access token created from an existing parent token. The restricted token has less access than the parent token from which it is copied and can be created by changing one or more security identifiers that allow access in the parent token and not in the restricted token. The restricted token can also be created by removing one or more privileges from the restricted token which are present in the parent token.

A security context is set up for the user when the user logs on to the system and is authenticated. The access token is made which includes user and groups field, security identifier (security ID) based on user's credential and on basis of one or more group within the organization. When the user tries to start a process on a resource the kernel that is associated with the resource mode security compares the user's access to the action and the list of actions

Fig. 3, represents the invention as taught by Jensenworth, a process 70 desiring access to an object 72 acquires the type of access it is granted (e.g., may be read and write for a word document). The kernel provides an associated token to the object manager 74. The object 72 has a security descriptor 76 and the token 60 to the security mechanism 78. The contents of the security descriptors are determined by the owner of the object and comprises of access control list (ACL) which has the information about the access rights allowed to the token in form of a bitmask where each bit corresponds to permission (one bit is for read, the other one bit is for write etc). The security mechanism compares the security IDs in the token 60 with the action requested by the process 70 against the entries in ACL 80. If it is found that the user can be allowed access then a handle to the object is returned to the process else the access is denied.

The SACL 81 includes an audit entry having a group security identifier. It logs any failed attempt to write to a file object. The security descriptor 76 consists of a list of ID's with the type of access allowed. For example, RO indicates read only, WR means both read and write access etc.

Independent claim 1, recites "[a] kernel-level transaction system, comprising:

> a memory;
>
> one or more processors operatively coupled to the memory;
>
> plural kernel objects to implement a transaction having plural operations; and
>
> a security descriptor, applied to at least one of the kernel objects, to identify at least one user, to identify one of the operations of the transaction that may be performed on the kernel object to which the security descriptor is applied, and to identify a right indicating that the identified user is permitted or prohibited to perform the operation.

Jensenworth does not teach or show "one of the operations of the transaction that may be performed on the kernel object to which the security descriptor is applied" as recited in claim 1. As discussed above, Jensenworth teaches a security model using restricted tokens. When a process starts, the kernel mode security mechanism first compares the user based security identifiers and intended type of action against a list of identifiers that is associated with the source. Jensenworth shows that the kernel objects are used only for the identification of the correct user as per security requirements. An object manager is also described that handles the associated token provided by the kernel. The kernel object includes the security descriptor that only performs the identification check but the transaction process is carried out outside the kernel object.

On the other hand, the application describes one of the operations of the transaction that may be performed on the kernel object to which the security descriptor is applied. The application describes a transaction management functionality implemented by kernel objects. The kernel objects further include a transaction object, a resource management object and an enlistment object. Thereofore, the application describes that complete transaction process is carried out by Kernel objects.

Accordingly, Jensenworth does not show every element of claim 1, and the rejection of claim 1 is therefore improper. Accordingly, Applicant respectfully request that the §102 rejection of claim 1 be withdrawn.

Dependent claims 2-6 depend from claim 1, and are allowable at the least for reasons provided in support of claim 1. Accordingly, Applicant respectfully request that the §102 rejection of claims 2-6 be withdrawn.

Claim 2 further recites "a transaction object to represent a transaction; a resource manager object to represent a resource participating in the transaction; and an enlistment object to enlist participants in the transaction."

Jensenworth fails to teach or show "the plural kernel objects include: a transaction object to represent a transaction; a resource manager object to represent a resource participating in the transaction; and an enlistment object to enlist participants in the transaction" as recited in claim 2. Jensenworth teaches a security model using restricted tokens. When a process starts, the kernel mode security mechanism first compares the user based security identifiers and intended type of action against a list of identifiers that is associated with the source. Jensenworth teaches that the kernel objects are used only for the identification of the correct user as per security requirements. An object manager is taught that handles the associated token provided by the kernel. The kernel object includes the security descriptor that only performs the identification check, but the transaction process is carried out outside the kernel object.

The application shows a transaction management functionality implemented by kernel objects. The kernel objects further include a transaction object, a resource management object and an enlistment object. The application describes that complete transaction process is carried out by kernel objects.

Claim 6 further recites "and the operation identified by the security descriptor includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, determine a state of enlistments at a moment of transaction failure, obtain and reference an enlistment key, rollback the transaction and to respond to notifications, and perform operations a superior transaction manager would perform."

Jensenworth does not teach or show this element. Jensenworth teaches that a user is allotted a restricted token and whenever the user logs in a check is made to determine if the user has that restricted token or the parent token. If the token is the restricted token, then another check is made to determine what all privileges are given to the user by comparing the restricted with a list of already defined rights. If both the checks are cleared then only the user gets the right to access data, otherwise the access is denied. Jensenworth does not teach or show that the process that has to be followed if a transaction fails or is interrupted.

The application describes that whenever an operation fails, then all the operations that are being performed are stopped and the data that is being transferred gets stored. The transaction is rolled back and notifications are sent.

Independent claim 7 recites "[a] method of implementing a kernel-level transaction, comprising:

attaching a security descriptor to at least one of plural kernel objects utilized in a transaction; and

performing an operation for a transaction on the at least one kernel object in accordance with the rights accorded by the security descriptor attached to the at least one kernel object.

Jensenworth does not teach or show "performing an operation for a transaction on the at least one kernel object in accordance with the rights accorded by the security descriptor attached to the at least one kernel object" as recited in claim 7. Claim 7 benefits from similar arguments presented in support of claim 1.

Accordingly, Jensenworth does not show every element of claim 7, and the rejection of claim 7 is therefore improper. Accordingly, Applicant respectfully request that the §102 rejection of claim 7 be withdrawn.

Dependent claims 8-14 depend from claim 7, and are allowable at the least for reasons provided in support of claim 7. Accordingly, Applicant respectfully request that the §102 rejection of claims 8-14 be withdrawn.

Claim 14 further benefits from reasons provided in support of claim 6.

Independent claim 15 recites "[a] computer-readable medium having stored thereon an object attached to a kernel object, the object comprising:

a first data entry identifying at least one user;

a second data entry identifying an operation capable of being performed on the kernel object by the user identified by the first data entry; and a third data entry indicating a right for the user identified by the first data entry to perform the operation identified by the second data entry.

Jensenworth does not teach or show "identifying an operation capable of being performed on the kernel object" as recited in claim 15. Claim 15 benefits from similar arguments presented in support of claim 1.

Accordingly, Jensenworth does not show every element of claim 15, and the rejection of claim 15 is therefore improper. Accordingly, Applicant respectfully request that the §102 rejection of claim 15 be withdrawn.

Dependent claims 16-18 depend from claim 15, and are allowable at the least for reasons provided in support of claim 15. Accordingly, Applicant respectfully request that the §102 rejection of claims 16-18 be withdrawn.

Claim 18 further benefits from reasons provided in support of claim 6.

Independent claim 19 recites "[a] transaction method, comprising:

implementing a transaction among kernel objects; and

securing the transaction utilizing an operating system security model that applies a security descriptor to at least one of the kernel objects participating in the transaction.

Jensenworth does not teach or show "applyies a security descriptor to at least one of the kernel objects participating in the transaction", as recited in claim 19. Jensenworth teaches a security model using restricted tokens. When a process starts, the kernel mode security mechanism first compares the user based security identifiers and intended type of action against a list of identifiers that is associated with the source. Jensenworth describes that the kernel objects are used only for the identification of the correct user as per security requirements. An object manager is described that handles the associated token provided by the kernel. The kernel object includes the security descriptor that only performs the identification check but the transaction process is carried out outside the kernel object.

The application describes one of the operations of the transaction that may be performed on the kernel object to which the security descriptor is applied. The application describes a transaction management functionality implemented by kernel objects. The kernel objects further include a transaction object, a resource management object and an enlistment object. Therefore, the application describes that complete transaction process is carried out by Kernel objects.

Accordingly, Jensenworth does not show every element of claim 19, and the rejection of claim 19 is therefore improper. Accordingly, Applicant respectfully request that the §102 rejection of claim 19 be withdrawn.

Dependent claim 20 depends from claim 19, and is allowable at the least for reasons provided in support of claim 19. Accordingly, Applicant respectfully request that the §102 rejection of claim 20 be withdrawn.

Independent claim 21 recites "[a] method of implementing a transaction, comprising:

> attaching a security descriptor to at least one of plural objects utilized in a transaction; and
>
> performing an operation for a transaction on the at least one object in accordance with the rights accorded by the security descriptor attached to the at least one object.

Jensenworth does not teach or show "performing an operation for a transaction on the at least one object in accordance with the rights accorded by the security descriptor attached to the at least one object" as recited in claim 21. Claim 21 benefits from similar arguments presented in support of claim 1.

Accordingly, Jensenworth does not show every element of claim 21, and the rejection of claim 21 is therefore improper. Accordingly, Applicant respectfully request that the §102 rejection of claim 21 be withdrawn.

Dependent claims 22-28 depend from claim 21, and are allowable at the least for reasons provided in support of claim 21. Accordingly, Applicant respectfully request that the §102 rejection of claims 22-28 be withdrawn.

Claim 28 further benefits from reasons provided in support of claim 6.

Independent claim 29 recites "[a] kernel-level transaction system, comprising:

> a memory;
>
> one or more processors operatively coupled to the memory;
>
> means for implementing a transaction among kernel objects; and
>
> means for securing the transaction by applying a security descriptor to at least one of the kernel objects,
>
> wherein the security descriptor identifies at least one user, an operation to be performed on the kernel object to which the security descriptor is applied, and a right indicating that the identified user is permitted or prohibited to perform the operation.

Jensenworth does not teach or show "means for securing the transaction by applying a security descriptor to at least one of the kernel objects, wherein the security descriptor identifies at least one user, an operation to be performed on the kernel object to which the security descriptor is applied" as recited in claim 29. Claim 29 benefits from similar arguments presented in support of claim 1.

Accordingly, Jensenworth does not show every element of claim 29, and the rejection of claim 29 is therefore improper. Accordingly, Applicant respectfully request that the §102 rejection of claim 29 be withdrawn.

Dependent claims 30-33 depend from claim 29, and are allowable at the least for reasons provided in support of claim 29. Accordingly, Applicant respectfully request that the §102 rejection of claims 30-33 be withdrawn.

Claim 30 further benefits from reasons provided in support of claim 6.

CONCLUSION

All pending claims 1-33 are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the subject application. If any issues remain that prevent issuance of this application, the Examiner is urged to contact the undersigned attorney before issuing a subsequent Action.

Respectfully Submitted,

Dated: September 4, 2007

By: /Emmanuel A. Rivera/
Emmanuel A. Rivera
Reg. No. 45,760
(509) 324-9256 ext. 245